



PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the application of)
Kazuhito GASSHO et al.)
Application No. 10/722,693)
Filed: November 24, 2003)
For: PRINTER AND PRINT SYSTEM)

Examiner: Not Assigned
Art Unit: 2854
Docket No. KYWAP006
Date: April 26, 2004

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class Mail in an envelope addressed to: Commissioner for Patents, Alexandria, VA 22313-1450 on April 26, 2004.

Signed:


Diane Schwanbeck

SUBMISSION OF PRIORITY DOCUMENTS

Commissioner for Patents
Alexandria, Virginia 22313-1450

Sir:

Applicants have claimed the benefit of the filing dates of: 1) Japanese Patent Application No. 2002-343873, filed on November 27, 2002; 2) Japanese Patent Application No. 2002-343905, filed on November 27, 2002; 3) Japanese Patent Application No. 2003-300445, filed on August 25, 2003; and 4) Japanese Patent Application No. 2003-300458, filed on August 25, 2003, under 35 U.S.C. § 119. In compliance with 35 U.S.C. § 119(b), Applicants are attaching certified copies of these four (4) Japanese priority applications.

Respectfully submitted,
MARTINE & PENILLA, LLP



Peter B. Martine
Reg. No. 32,043

710 Lakeway Drive, Suite 170
Sunnyvale, CA 94085
Telephone: (408) 749-6900
Customer No. 25920

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 2002年11月27日
Date of Application:

出願番号 特願2002-343873
Application Number:

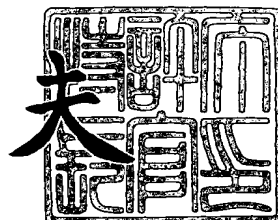
[ST. 10/C]: [JP 2002-343873]

出願人 セイコーエプソン株式会社
Applicant(s):

2004年 1月 7日

特許庁長官
Commissioner,
Japan Patent Office

今井 康夫



U.S. Application No. 10/722,693

出証番号 出証特2003-3109252

【書類名】 特許願

【整理番号】 13952801

【提出日】 平成14年11月27日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 3/12

【発明の名称】 プリンタ及び印刷システム

【請求項の数】 10

【発明者】

 【住所又は居所】 長野県諏訪市大和三丁目3番5号 セイコーエプソン株式会社内

 【氏名】 合 掌 和 人

【発明者】

 【住所又は居所】 長野県諏訪市大和三丁目3番5号 セイコーエプソン株式会社内

 【氏名】 島 敏 博

【発明者】

 【住所又は居所】 長野県諏訪市大和三丁目3番5号 セイコーエプソン株式会社内

 【氏名】 小 嶋 輝 人

【特許出願人】

 【識別番号】 000002369

 【住所又は居所】 東京都新宿区西新宿二丁目4番1号

 【氏名又は名称】 セイコーエプソン株式会社

【代理人】

 【識別番号】 100075812

 【弁理士】

 【氏名又は名称】 吉 武 賢 次

【選任した代理人】

【識別番号】 100088889

【弁理士】

【氏名又は名称】 橋 谷 英 俊

【選任した代理人】

【識別番号】 100082991

【弁理士】

【氏名又は名称】 佐 藤 泰 和

【選任した代理人】

【識別番号】 100096921

【弁理士】

【氏名又は名称】 吉 元 弘

【選任した代理人】

【識別番号】 100103263

【弁理士】

【氏名又は名称】 川 崎 康

【選任した代理人】

【識別番号】 100107582

【弁理士】

【氏名又は名称】 関 根 毅

【手数料の表示】

【予納台帳番号】 087654

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 プリンタ及び印刷システム

【特許請求の範囲】

【請求項 1】

当該プリンタの設置されている場所を特定するためのプリンタ位置情報を取得する、プリンタ位置情報取得手段と、

正当な権限を有する者が要求した場合に、前記プリンタ位置情報取得手段からプリンタ位置情報を取得し、これを第 1 プリンタ位置情報とするとともに、前記第 1 プリンタ位置情報を少なくとも含むパスフレーズを用いて、公開鍵を生成する、公開鍵生成手段と、

前記公開鍵生成手段で生成した公開鍵が格納される、公開鍵格納手段と、

前記公開鍵で暗号化された印刷データを受信する、印刷データ受信手段と、

前記印刷データを受信した際に、前記プリンタ位置情報取得手段からプリンタ位置情報を取得し、これを第 2 プリンタ位置情報とする、第 2 プリンタ位置情報取得手段と、

前記第 2 プリンタ位置情報を少なくとも含むパスフレーズを用いて、秘密鍵を生成する、秘密鍵生成手段と、

前記秘密鍵を用いて、前記印刷データ受信手段で受信した前記印刷データを復号する、復号手段と、

を備えることを特徴とするプリンタ。

【請求項 2】

印刷クライアントから公開鍵取得要求を受信する、公開鍵取得要求受信手段と、

前記公開鍵格納手段に格納されている前記公開鍵を読み出して、前記公開鍵取得要求を送信した印刷クライアントに送信する、公開鍵送信手段と、

をさらに備えることを特徴とする請求項 1 に記載のプリンタ。

【請求項 3】

当該プリンタの設置されている場所を特定するためのプリンタ位置情報を取得する、プリンタ位置情報取得手段と、

正当な権限を有する者が要求した場合に、前記プリンタ位置情報取得手段からプリンタ位置情報を取得し、これを第 1 プリンタ位置情報とするとともに、前記第 1 プリンタ位置情報をプリンタ位置情報格納手段に格納する、第 1 プリンタ位置情報取得格納手段と、

前記プリンタ位置情報格納手段から前記第 1 プリンタ位置情報を読み出して、前記第 1 プリンタ位置情報を少なくとも含むパスフレーズを用いて、公開鍵を生成する、公開鍵生成手段と、

前記公開鍵で暗号化された印刷データを受信する、印刷データ受信手段と、

前記印刷データを受信した際に、前記プリンタ位置情報取得手段からプリンタ位置情報を取得し、これを第 2 プリンタ位置情報とする、第 2 プリンタ位置情報取得手段と、

前記第 2 プリンタ位置情報を少なくとも含むパスフレーズを用いて、秘密鍵を生成する、秘密鍵生成手段と、

前記秘密鍵を用いて、前記印刷データ受信手段で受信した前記印刷データを復号する、復号手段と、

を備えることを特徴とするプリンタ。

【請求項 4】

印刷クライアントから公開鍵取得要求を受信する、公開鍵取得要求受信手段をさらに備えるとともに、

前記公開鍵生成手段は、前記公開鍵取得要求受信手段が公開鍵取得要求を受信した際に、公開鍵を生成する、

ことを特徴とする請求項 3 に記載のプリンタ。

【請求項 5】

前記公開鍵生成手段が生成した前記公開鍵を、前記公開鍵取得要求を送信した印刷クライアントに送信する、公開鍵送信手段を、

さらに備えることを特徴とする請求項 4 に記載のプリンタ。

【請求項 6】

操作者に認証情報を要求する、認証情報要求手段と、

認証情報が入力された場合に、入力された認証情報が登録されている認証情報

と一致するかどうかを判断し、両者が一致した場合には、操作者が正当な権限を有する者であると判断する、認証判断手段と、

をさらに備えることを特徴とする請求項 1 乃至請求項 5 のいずれかに記載のプリンタ。

【請求項 7】

前記公開鍵生成手段が公開鍵を生成する際に、秘密鍵が生成された場合でも、この秘密鍵は破棄する、ことを特徴とする請求項 6 に記載のプリンタ。

【請求項 8】

前記秘密鍵を用いて前記印刷データが復号できた場合には、前記印刷データに基づく印刷を実行し、前記秘密鍵を用いて前記印刷データが復号できなかった場合には、前記印刷データに基づく印刷を実行しない、選択印刷実行手段を、さらに備えることを特徴とする請求項 7 に記載のプリンタ。

【請求項 9】

プリンタと印刷クライアントとを有する、印刷システムであって、

前記プリンタは、

当該プリンタの設置されている場所を特定するためのプリンタ位置情報を取得する、プリンタ位置情報取得手段と、

正当な権限を有する者が要求した場合に、前記プリンタ位置情報取得手段からプリンタ位置情報を取得し、これを第 1 プリンタ位置情報とするとともに、前記第 1 プリンタ位置情報を少なくとも含むパスフレーズを用いて、公開鍵を生成する、公開鍵生成手段と、

前記公開鍵生成手段で生成した公開鍵が格納される、公開鍵格納手段と、

を備えており、

前記印刷クライアントは、

前記プリンタで印刷を行うための印刷データを生成する、印刷データ生成手段と、

前記公開鍵で前記印刷データを暗号化し、この暗号化した印刷データを、前記プリンタに送信する、印刷データ送信手段と、

を備えており、

前記プリンタは、さらに、
前記公開鍵で暗号化された印刷データを受信する、印刷データ受信手段と、
前記印刷データを受信した際に、前記プリンタ位置情報取得手段からプリンタ位置情報を取得し、これを第2プリンタ位置情報とする、第2プリンタ位置情報取得手段と、

前記第2プリンタ位置情報を少なくとも含むパスフレーズを用いて、秘密鍵を生成する、秘密鍵生成手段と、

前記秘密鍵を用いて、前記印刷データ受信手段で受信した前記印刷データを復号する、復号手段と、

を備えることを特徴とする印刷システム。

【請求項10】

プリンタと印刷クライアントとを有する、印刷システムであって、

前記プリンタは、

当該プリンタの設置されている場所を特定するためのプリンタ位置情報を取得する、プリンタ位置情報取得手段と、

正当な権限を有する者が要求した場合に、前記プリンタ位置情報取得手段からプリンタ位置情報を取得し、これを第1プリンタ位置情報とするとともに、前記第1プリンタ位置情報をプリンタ位置情報格納手段に格納する、第1プリンタ位置情報取得格納手段と、

前記プリンタ位置情報格納手段から前記第1プリンタ位置情報を読み出して、前記第1プリンタ位置情報を少なくとも含むパスフレーズを用いて、公開鍵を生成する、公開鍵生成手段と、

を備えており、

前記印刷クライアントは、

前記プリンタで印刷を行うための印刷データを生成する、印刷データ生成手段と、

前記公開鍵で前記印刷データを暗号化し、この暗号化した印刷データを、前記プリンタに送信する、印刷データ送信手段と、

を備えており、

前記プリンタは、さらに、
前記公開鍵で暗号化された印刷データを受信する、印刷データ受信手段と、
前記印刷データを受信した際に、前記プリンタ位置情報取得手段からプリンタ位置情報を取得し、これを第 2 プリンタ位置情報とする、第 2 プリンタ位置情報取得手段と、

前記第 2 プリンタ位置情報を少なくとも含むパスフレーズを用いて、秘密鍵を生成する、秘密鍵生成手段と、

前記秘密鍵を用いて、前記印刷データ受信手段で受信した前記印刷データを復号する、復号手段と、

を備えることを特徴とする印刷システム。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、プリンタ及び印刷システムに関し、特に、印刷できる場所を制限したプリンタ及び印刷システムに関する。

【0 0 0 2】

【従来の技術】

近年、プリンタを用いたビジネスモデルとして、プリンタメーカーがユーザにプリンタを無償で貸し出し、ユーザがこのプリンタを用いて印刷した枚数だけ、そのプリンタメーカーに使用料を支払うという形態が、注目されてきている。このようなビジネスモデルにおいては、印刷枚数に応じた課金の他に、使用期間に応じた課金や、使用インク量に応じた課金などが考えられる。

【0 0 0 3】

【特許文献 1】

特開平 1 1 - 3 3 1 1 4 4 号公報

【0 0 0 4】

【発明が解決しようとする課題】

しかしながら、このようなビジネスモデルでは、プリンタメーカーから貸し出されたプリンタを、ユーザが無断で転売したり、他人に貸し出したりしてしまうと

、プリンタメーカーがプリンタの使用に応じた課金をすることができなくなってしまう。このため、プリンタメーカーとしては、貸し出したプリンタが使用できる場所、つまり、正常な印刷ができる場所を、その貸し出したユーザの場所に限定したい。

【0005】

そこで本発明は、前記課題に鑑みてなされたものであり、予め登録した場所では正常に印刷することのできないプリンタ及び印刷システムを提供することを目的とする。

【0006】

【課題を解決するための手段】

上記課題を解決するため、本発明に係るプリンタは、当該プリンタの設置されている場所を特定するためのプリンタ位置情報を取得する、プリンタ位置情報取得手段と、正当な権限を有する者が要求した場合に、前記プリンタ位置情報取得手段からプリンタ位置情報を取得し、これを第1プリンタ位置情報とするとともに、前記第1プリンタ位置情報を少なくとも含むパスフレーズを用いて、公開鍵を生成する、公開鍵生成手段と、前記公開鍵生成手段で生成した公開鍵が格納される、公開鍵格納手段と、前記公開鍵で暗号化された印刷データを受信する、印刷データ受信手段と、前記印刷データを受信した際に、前記プリンタ位置情報取得手段からプリンタ位置情報を取得し、これを第2プリンタ位置情報とする、第2プリンタ位置情報取得手段と、前記第2プリンタ位置情報を少なくとも含むパスフレーズを用いて、秘密鍵を生成する、秘密鍵生成手段と、前記秘密鍵を用いて、前記印刷データ受信手段で受信した前記印刷データを復号する、復号手段と、を備えることを特徴とする。

【0007】

この場合、印刷クライアントから公開鍵取得要求を受信する、公開鍵取得要求受信手段と、前記公開鍵格納手段に格納されている前記公開鍵を読み出して、前記公開鍵取得要求を送信した印刷クライアントに送信する、公開鍵送信手段と、をさらに備えるようにしてもよい。

【0008】

また、本発明に係るプリンタは、当該プリンタの設置されている場所を特定するためのプリンタ位置情報を取得する、プリンタ位置情報取得手段と、正当な権限を有する者が要求した場合に、前記プリンタ位置情報取得手段からプリンタ位置情報を取得し、これを第 1 プリンタ位置情報とするとともに、前記第 1 プリンタ位置情報をプリンタ位置情報格納手段に格納する、第 1 プリンタ位置情報取得格納手段と、前記プリンタ位置情報格納手段から前記第 1 プリンタ位置情報を読み出して、前記第 1 プリンタ位置情報を少なくとも含むパスフレーズを用いて、公開鍵を生成する、公開鍵生成手段と、前記公開鍵で暗号化された印刷データを受信する、印刷データ受信手段と、前記印刷データを受信した際に、前記プリンタ位置情報取得手段からプリンタ位置情報を取得し、これを第 2 プリンタ位置情報とする、第 2 プリンタ位置情報取得手段と、前記第 2 プリンタ位置情報を少なくとも含むパスフレーズを用いて、秘密鍵を生成する、秘密鍵生成手段と、前記秘密鍵を用いて、前記印刷データ受信手段で受信した前記印刷データを復号する、復号手段と、を備えることを特徴とする。

【0 0 0 9】

この場合、印刷クライアントから公開鍵取得要求を受信する、公開鍵取得要求受信手段をさらに備えるとともに、前記公開鍵生成手段は、前記公開鍵取得要求受信手段が公開鍵取得要求を受信した際に、公開鍵を生成するようにしてもよい。

【0 0 1 0】

この場合、前記公開鍵生成手段が生成した前記公開鍵を、前記公開鍵取得要求を送信した印刷クライアントに送信する、公開鍵送信手段を、さらに備えるようにしてもよい。

【0 0 1 1】

上述したプリンタでは、操作者に認証情報を要求する、認証情報要求手段と、認証情報が入力された場合に、入力された認証情報が登録されている認証情報と一致するかどうかを判断し、両者が一致した場合には、操作者が正当な権限を有する者であると判断する、認証判断手段と、をさらに備えるようにしてもよい。

【0 0 1 2】

また、前記公開鍵生成手段が公開鍵を生成する際に、秘密鍵が生成された場合でも、この秘密鍵は破棄するようにしてもよい。

【 0 0 1 3 】

また、前記秘密鍵を用いて前記印刷データが復号できた場合には、前記印刷データに基づく印刷を実行し、前記秘密鍵を用いて前記印刷データが復号できなかった場合には、前記印刷データに基づく印刷を実行しない、選択印刷実行手段を、さらに備えるようにしてもよい。

【 0 0 1 4 】

本発明に係る印刷システムは、プリンタと印刷クライアントとを有する、印刷システムであって、前記プリンタは、当該プリンタの設置されている場所を特定するためのプリンタ位置情報を取得する、プリンタ位置情報取得手段と、正当な権限を有する者が要求した場合に、前記プリンタ位置情報取得手段からプリンタ位置情報を取得し、これを第 1 プリンタ位置情報とするとともに、前記第 1 プリンタ位置情報を少なくとも含むパスフレーズを用いて、公開鍵を生成する、公開鍵生成手段と、前記公開鍵生成手段で生成した公開鍵が格納される、公開鍵格納手段と、を備えており、前記印刷クライアントは、前記プリンタで印刷を行うための印刷データを生成する、印刷データ生成手段と、前記公開鍵で前記印刷データを暗号化し、この暗号化した印刷データを、前記プリンタに送信する、印刷データ送信手段と、を備えており、前記プリンタは、さらに、前記公開鍵で暗号化された印刷データを受信する、印刷データ受信手段と、前記印刷データを受信した際に、前記プリンタ位置情報取得手段からプリンタ位置情報を取得し、これを第 2 プリンタ位置情報とする、第 2 プリンタ位置情報取得手段と、前記第 2 プリンタ位置情報を少なくとも含むパスフレーズを用いて、秘密鍵を生成する、秘密鍵生成手段と、前記秘密鍵を用いて、前記印刷データ受信手段で受信した前記印刷データを復号する、復号手段と、を備えることを特徴とする。

【 0 0 1 5 】

本発明に係る印刷システムは、プリンタと印刷クライアントとを有する、印刷システムであって、前記プリンタは、当該プリンタの設置されている場所を特定するためのプリンタ位置情報を取得する、プリンタ位置情報取得手段と、正当な

権限を有する者が要求した場合に、前記プリンタ位置情報取得手段からプリンタ位置情報を取得し、これを第1プリンタ位置情報とするとともに、前記第1プリンタ位置情報をプリンタ位置情報格納手段に格納する、第1プリンタ位置情報取得格納手段と、前記プリンタ位置情報格納手段から前記第1プリンタ位置情報を読み出して、前記第1プリンタ位置情報を少なくとも含むパスフレーズを用いて、公開鍵を生成する、公開鍵生成手段と、を備えており、前記印刷クライアントは、前記プリンタで印刷を行うための印刷データを生成する、印刷データ生成手段と、前記公開鍵で前記印刷データを暗号化し、この暗号化した印刷データを、前記プリンタに送信する、印刷データ送信手段と、を備えており、前記プリンタは、さらに、前記公開鍵で暗号化された印刷データを受信する、印刷データ受信手段と、前記印刷データを受信した際に、前記プリンタ位置情報取得手段からプリンタ位置情報を取得し、これを第2プリンタ位置情報とする、第2プリンタ位置情報取得手段と、前記第2プリンタ位置情報を少なくとも含むパスフレーズを用いて、秘密鍵を生成する、秘密鍵生成手段と、前記秘密鍵を用いて、前記印刷データ受信手段で受信した前記印刷データを復号する、復号手段と、を備えることを特徴とする。

【0016】

なお、本発明は、プリンタを制御するための制御方法、及び、印刷システムを制御するための制御方法として実現することもできる。さらには、そのようにプリンタ、及び、印刷システムを制御するためのプログラムやそのプログラムを記録した記録媒体として実現することもできる。

【0017】

【発明の実施の形態】

〔第1実施形態〕

第1実施形態に係る印刷システムは、プリンタがその時点で設置されている位置を表すプリンタ位置情報を少なくとも含むパスフレーズを用いて公開鍵を生成し、この公開鍵をプリンタに格納しておく。この公開鍵の生成は、公開鍵生成認証情報が一致した特定の者が要求した場合にのみ、プリンタで実行される。

【0018】

そして、印刷クライアントから公開鍵の送信を要求された場合には、プリンタは、格納しておいた公開鍵を読み出して、印刷クライアントに送信する。印刷クライアントが印刷データをこのプリンタに送信する際には、この取得した公開鍵を用いて印刷データを暗号化して生成した印刷送信用データとして送信する。この印刷送信用データを受信したプリンタでは、受信時に再度、その時点におけるプリンタ位置情報を少なくとも含むパスフレーズを用いて秘密鍵を生成し、この秘密鍵で印刷送信用データが復号できた場合にのみ印刷を実行する。このようにすることにより、正当な権限のある者がプリンタに公開鍵を登録した位置でしか、正常な印刷ができないようにしたものである。より詳しくを、以下に説明する。

【0019】

まず、図1に基づいて、本実施形態に係る印刷システムの構成を説明する。図1は、本実施形態に係る印刷システムのハードウェア構成を示すブロック図である。

【0020】

この図1に示すように、本実施形態に係る印刷システムは、プリンタケーブル10を介して接続された印刷クライアント20とプリンタ30とを備えている。すなわち、プリンタ30は印刷クライアント20にローカル接続されている。但し、印刷クライアント20とプリンタ30との間は、無線やイーサネット（登録商標）等を用いたネットワークにより接続されるようにしてもよい。この場合には、1つのプリンタ30に複数の印刷クライアント20が接続されてもよい。

【0021】

印刷クライアント20は、例えば、ホストコンピュータやパーソナルコンピュータと呼ばれる各種のコンピュータにより構成されている。本実施形態では、特に印刷クライアント20は、印刷データを公開鍵で暗号化した印刷送信用データを生成し、この印刷送信用データをプリンタケーブル10を介してプリンタ30に送信する。また、この印刷クライアント20は、コンピュータに限られるものではなく、例えば、撮影した画像を印刷する必要があるデジタルカメラや、印刷画像データをコンテンツとして蓄積してあるコンテンツサーバ等でもよい。

【0022】

また本実施形態においては、プリンタ30は、正当な権限を有する者が操作した場合に限り、公開鍵暗号法により公開鍵を生成することができるプリンタである。生成した公開鍵は、このプリンタ30に格納され、保持される。そして、プリンタ30は、印刷送信用データを印刷クライアント20から受信し、この印刷送信用データを、少なくともその時点のプリンタ位置情報を含むパズフレーズを用いて生成した秘密鍵で、復号する。そして、印刷送信用データの復号ができた場合には、その印刷送信用データに基づく印刷を行い、印刷送信用データの復号ができなかった場合には、その印刷送信用データに基づく印刷は行わない。

【0023】

また、本実施形態においては、プリンタ30は、公開鍵で暗号化されていない印刷データでは、正常な印刷結果が得られないように構成されている。すなわち、暗号化されていない印刷データは、プリンタ30では、秘密鍵を用いて復号できない印刷送信用データとして扱われる。

【0024】

図2は、プリンタ30の内部構成を説明するためのブロック図である。この図2に示すように、プリンタ30は、CPU (Central Processing Unit) 40と、RAM (Random Access Memory) 42と、ROM (Read Only Memory) 44と、EEPROM (Electrically Erasable Programmable ROM) 45を備えており、これらは互いに内部バス46を介して接続されている。また、この内部バス46には、通信用のインターフェース48が接続されており、この通信用のインターフェース48を介して、上述したプリンタケーブル10にプリンタ30が接続されている。さらに、内部バス46には、インターフェース50が接続されており、このインターフェース50には印刷エンジン52が接続されている。本実施形態においては、EEPROM45は、書き換え可能な不揮発性記憶装置として機能する。

【0025】

また、内部バス46には、位置検出部54が接続されている。この位置検出部54は、プリンタ30が設置されている位置を特定する機能を有する。本実施形

態においては、例えば、GPS (global positioning system) により構成されており、このプリンタ 3 0 が設置されている位置の緯度、経度、高度が特定できるようになっている。現時点におけるGPSの精度は、緯度、経度、高度において、それぞれ±10 m程度であると言われている。

【0 0 2 6】

但し、この位置検出部 5 4 は、GPSを用いた構成に限らず、例えば、PHS (Personal Handyphone System) などの移動体通信技術を利用して、プリンタ 3 0 の位置を特定するようにしてもよい。

【0 0 2 7】

さらに、内部バス 4 6 には、インターフェース 5 6 を介して、ハードディスク 5 8 が接続されている。本実施形態においては、このハードディスク 5 8 は、書き換え可能な不揮発性記憶装置として機能する。

【0 0 2 8】

図 3 は、印刷クライアント 2 0 の内部構成を説明するためのブロック図である。この図 3 に示すように、本実施形態に係る印刷クライアント 2 0 は、コンピュータ本体 6 0 とディスプレイ 6 2 とを備えて構成されている。

【0 0 2 9】

コンピュータ本体 6 0 は、CPU 6 4 と、RAM 6 6 と、ROM 6 8 とを備えており、これらは互いに内部バス 7 0 を介して接続されている。また、この内部バス 7 0 には、通信用のインターフェース 7 2 が接続されており、この通信用のインターフェース 7 2 を介して、上述したプリンタケーブル 1 0 に印刷クライアント 2 0 が接続されている。

【0 0 3 0】

さらに、内部バス 7 0 には、インターフェース 7 4 が接続されており、このインターフェース 7 4 には大容量記憶装置であるハードディスク 7 6 が接続されている。本実施形態においては、このハードディスク 7 6 は、書き換え可能な不揮発性記憶装置として機能する。また、内部バス 7 0 には、インターフェース 7 8 が接続されており、このインターフェース 7 8 から延びるケーブル 8 0 を介して、上述したディスプレイ 6 2 が接続されている。

【 0 0 3 1 】

次に、本実施形態に係る印刷システムにおいて、印刷クライアント 2 0 がプリンタ 3 0 で印刷を行う場合の処理を、概略的に説明する。

【 0 0 3 2 】

本実施形態においては、プリンタ 3 0 は、正当な権限のある者の要求に基づいて公開鍵を生成し、E E P R O M 4 5 に格納する。本実施形態においては、正当な権限のある者であるかどうかは、プリンタ 3 0 のコントロールパネルから、操作者に公開鍵生成認証情報を入力させることにより、判断する。また、本実施形態においては、この公開鍵生成認証情報は、I D とパスワードの組み合わせから構成されている。また、公開鍵生成認証情報の入力、印刷クライアント 2 0 で入力させて、プリンタケーブル 1 0 を介して、プリンタ 3 0 に送信するようにしてもよい。また、プリンタ 3 0 がネットワークプリンタである場合には、このネットワークを介して、別の場所から公開鍵生成認証情報をこのプリンタ 3 0 に送信するようにしてもよい。

【 0 0 3 3 】

プリンタ 3 0 では、このプリンタ 3 0 の設置されている位置を示すプリンタ位置情報を少なくとも含むパスフレーズを用いて、公開鍵を、公開鍵暗号法により生成する。但し、この際、秘密鍵は生成しないか、生成されたとしても破棄する。そして、プリンタ 3 0 は、印刷クライアント 2 0 から公開鍵取得要求を受け付けた場合には、この公開鍵をE E P R O M 4 5 から読み出して、プリンタケーブル 1 0 を介して印刷クライアント 2 0 に送信する。

【 0 0 3 4 】

但し、プリンタ 3 0 の公開鍵は、必ずしもプリンタケーブル 1 0 を介して印刷クライアント 2 0 に通知する必要はない。例えば、印刷クライアント 2 0 のユーザが、正当な権限を有する者であれば、プリンタ 3 0 を操作することができるのであるから、ユーザがプリンタ 3 0 のコントロールパネルを操作して、プリンタ 3 0 の公開鍵を取得するようにしてもよい。この場合、ユーザはプリンタ 3 0 の公開鍵をフレキシブルディスク等の記録媒体に記録し、これを印刷クライアント 2 0 に読み込ませてもよい。

【0035】

次に、印刷クライアント20のユーザは、図4に示すように、印刷すべきデータである印刷データD05を作成し、印刷クライアント20に対してプリンタ30を指定して印刷を指示する。

【0036】

印刷クライアント20は、印刷データD05を、予め取得しておいたプリンタ30の公開鍵を用いて暗号化し、印刷送信用データD10を生成する。ここで、印刷データD05は、プリンタ30で印刷エンジン52を駆動した印刷を行うのに必要となる本来の印刷データを示している。なお、印刷送信用データD10は、この図4に示した印刷データD05以外のデータを含んでいてもよい。

【0037】

この印刷送信用データD10を受信したプリンタ30は、図2に示すように、この受信した印刷送信用データD10をRAM42に一旦格納する。そして、プリンタ30は、この暗号化された印刷送信用データD10を、秘密鍵を用いて復号する。すなわち、プリンタ30は、その時点におけるプリンタ位置情報を少なくとも含むパスフレーズを用いて、公開鍵暗号法により、秘密鍵を生成する。このように、印刷送信用データD10の復号を行おうとする度に、秘密鍵を生成することにより、このプリンタ30の設置場所が移動された場合には、移動前に生成された公開鍵で暗号化された印刷送信用データが、移動後のプリンタ30で復号できないようにしている。

【0038】

続いて、プリンタ30は、印刷送信用データD10が復号できたかどうかを判断する。印刷送信用データD10の復号ができた場合には、印刷送信用データD10を復号することにより取得した印刷データD05に基づいて印刷を行い、復号できなかった場合には、印刷は行わない。

【0039】

次に、上述した処理の内容について、フローチャートを用いて詳しく説明する。図5は、プリンタ30で実行される公開鍵生成処理を説明するフローチャートである。この公開鍵生成処理は、プリンタ30のROM44又はハードディスク

58に格納されている公開鍵生成プログラムをCPU40が読み込んで実行することにより実現される処理である。また、本実施形態においては、この公開鍵生成処理は、操作者（例えば、プリンタ30のメーカーのメンテナンスをする者）がプリンタ30のコントロールパネルを操作して、公開鍵生成処理を実行するように指示した場合に、起動され、実行される処理である。

【0040】

図5に示すように、公開鍵生成処理が実行された場合、プリンタ30はまず、操作者に、公開鍵生成認証情報を入力するように要求する（ステップS46）。本実施形態においては、操作者は、プリンタ30のコントロールパネルから、IDとパスワードを公開鍵生成認証情報として入力する。

【0041】

次に、プリンタ30は、公開鍵生成認証情報が入力されたかどうかを判断する（ステップS48）。この公開鍵生成認証情報が入力されていない場合（ステップS48：No）には、ステップS48の処理を繰り返して待機する。

【0042】

一方、公開鍵生成認証情報が入力された場合（ステップS48：Yes）には、入力された公開鍵生成認証情報が、登録されている公開鍵生成認証情報と一致するかどうかを判断する（ステップS50）。本実施形態においては、登録された公開鍵生成認証情報は、ROM44、EEPROM45、又は、ハードディスク58などに予め格納されている。このため、プリンタ30は、格納されている公開鍵生成認証情報を読み出して、操作者が入力した公開鍵生成認証情報と一致するかどうかを判断する。具体的には、登録されているID及びパスワードが、操作者が入力したID及びパスワードと一致するかどうかを判断する。

【0043】

公開鍵生成認証情報が一致しなかった場合（ステップS50：No）には、新たに公開鍵を生成することなく、この公開鍵生成処理を終了する。

【0044】

一方、公開鍵生成認証情報が一致した場合（ステップS50：Yes）には、プリンタ30は、このプリンタ30の機器固有情報を取得する（ステップS52

）。ここで、機器固有情報とは、このプリンタ 30 に関して、固有に割り当てられている識別情報であり、例えば、プリンタ 30 の製造シリアルナンバー、MAC アドレス等がある。

【0045】

次に、プリンタ 30 は、位置検出部 54 から、その時点におけるプリンタ 30 のプリンタ位置情報を取得する（ステップ S54）。これにより、プリンタ 30 のその時点における設置位置に関する情報を取得することができる。

【0046】

次に、プリンタ 30 は、機器固有情報とプリンタ位置情報とを用いてパズフレーズを作成する（ステップ S56）。このパズフレーズの作成手法は種々のものが考えられるが、本実施形態においては、単純に機器固有情報の後ろにプリンタ位置情報をつなげることにより、パズフレーズを作成する。なお、パズフレーズは、これら機器固有情報及びプリンタ位置情報以外のデータを含んでいてもよい。

【0047】

次に、プリンタ 30 は、ステップ S56 で作成したパズフレーズを用いて、公開鍵暗号法により、公開鍵を生成する（ステップ S58）。続いて、プリンタ 30 は、この生成した公開鍵を EEPROM 45 に格納する（ステップ S60）。図 6 は、EEPROM 45 の一部の領域に形成される公開鍵格納部 EP10 の構成を示す図である。この図 6 に示すように、公開鍵格納部 EP10 に、生成した公開鍵を格納して、保持する。なお、公開鍵を生成する際に、秘密鍵も生成された場合には、この秘密鍵は格納されずに破棄される。

【0048】

これにより、本実施形態に係る公開鍵生成処理が終了する。

【0049】

次に、公開鍵を印刷クライアント 20 が取得する場合における、印刷クライアント 20 及びプリンタ 30 の処理について説明する。

【0050】

図 7 は、印刷クライアント 20 で実行される公開鍵要求処理を説明するフロー

チャートである。この公開鍵要求処理は、印刷クライアントのROM 68又はハードディスク76に格納されている公開鍵要求プログラムをCPU 64が読み込んで実行することにより実現される処理である。また、本実施形態においては、この公開鍵要求処理は、ユーザが印刷クライアントに公開鍵を要求する処理を起動するように指示入力した場合に、起動され、実行される処理である。

【0051】

図7に示すように、この公開鍵要求処理においては、まず印刷クライアント20は、プリンタ30との接続を確立する（ステップS100）。続いて、印刷クライアント20は、プリンタ30へ認証情報を送信する（ステップS102）。本実施形態においては、この認証情報として、印刷クライアントを特定するための印刷クライアントIDと、パスワードとの組み合わせを用いている。したがって、印刷クライアント20は、印刷クライアントIDとパスワードとを、プリンタ30へ送信する。

【0052】

これに続いて、印刷クライアント20は、プリンタ30から認証が受け入れられたか否かを示す認証結果を受信するので、この認証結果に基づいて、プリンタ30で認証が認められたかどうかを判断する（ステップS104）。認証が認められなかった場合（ステップS104：No）には、上述したステップS102からを繰り返す。

【0053】

一方、認証が認められた場合（ステップS104：Yes）には、印刷クライアント20は、公開鍵取得要求をプリンタ30へ送信する（ステップS106）。そして、プリンタ30から公開鍵を受信したかどうかを判断する（ステップS108）。プリンタ30から公開鍵を受信していない場合（ステップS108：No）には、このステップS108を繰り返して待機する。

【0054】

一方、プリンタ30から公開鍵を受信した場合（ステップS108：Yes）には、この公開鍵を格納する（ステップS110）。本実施形態においては、印刷クライアント20は、ハードディスク76に公開鍵テーブルTB10を設けて

おり、取得した公開鍵は、この公開鍵テーブル T B 1 0 に格納され保持される。

【 0 0 5 5 】

図 8 は、この公開鍵テーブル T B 1 0 の構成の一例を示す図である。この図 8 に示すように、公開鍵テーブル T B 1 0 は、プリンタを特定するための情報を格納する項目 T D 1 0 と、取得した公開鍵をプリンタに対応させて格納する項目 T D 1 1 とを備えている。このように、公開鍵テーブル T B 1 0 は、複数のプリンタに関する公開鍵を、各プリンタ毎に保持することができるようになっている。また、このようにハードディスク 7 8 の公開鍵テーブル T B 1 0 に公開鍵を格納することにより、印刷クライアント 2 0 の電源がオフされて再び電源が投入された場合でも、それ以前に取得した公開鍵をそのままハードディスク 7 8 から読み出して使用することができるようになっている。

【 0 0 5 6 】

図 7 に示すように、次に、印刷クライアント 2 0 は、プリンタ 3 0 との接続を切断する（ステップ S 1 1 2）。これにより、図 7 に示した公開鍵要求処理は終了する。

【 0 0 5 7 】

次に、図 9 に基づいて、印刷クライアント 2 0 の公開鍵要求処理に対応して、プリンタ 3 0 で実行される公開鍵送信処理について説明する。この図 9 は、プリンタ 3 0 で実行される公開鍵送信処理を説明するフローチャートである。この公開鍵送信処理は、プリンタの R O M 4 4 又はハードディスク 5 8 に格納されている公開鍵送信プログラムを C P U 4 0 が読み込んで実行することにより実現される処理である。本実施形態においては、この公開鍵送信処理は、一定の時間間隔で定常的に実行されている処理である。また、この公開鍵送信処理は、上述した公開鍵要求処理に対応した処理である。

【 0 0 5 8 】

図 9 に示すように、プリンタ 3 0 は、印刷クライアント 2 0 からの接続を待っており、印刷クライアント 2 0 から接続を要求された場合に、印刷クライアント 2 0 と接続を確立する（ステップ S 1 2 0）。これは上述した印刷クライアント 2 0 側のステップ S 1 0 0 に対応している。続いて、プリンタ 3 0 は、印刷クラ

クライアント 2 0 から認証情報を受信したかどうかを判断する（ステップ S 1 2 2）。認証情報を受信していない場合（ステップ S 1 2 2 : N o）には、このステップ S 1 2 2 の処理を繰り返して待機する。

【 0 0 5 9 】

一方、認証情報を印刷クライアント 2 0 から受信した場合（ステップ S 1 2 2 : Y e s）には、その認証情報がこのプリンタ 3 0 に予め登録してある認証情報と一致するかどうかを判断する（ステップ S 1 2 4）。具体的には、上述したように、印刷クライアント 2 0 から印刷クライアント I D とパスワードが認証情報として送信されてくるので、この印刷クライアント I D とパスワードが、このプリンタ 3 0 に予め登録されている印刷クライアント I D とパスワードと一致するかどうかを判断する。

【 0 0 6 0 】

認証情報が一致しなかった場合（ステップ S 1 2 4 : N o）には、プリンタ 3 0 は印刷クライアント 2 0 に、認証が受け入れられなかった旨の認証結果を送信し（ステップ S 1 2 6）、後述するステップ S 1 3 6 において、印刷クライアント 2 0 との接続を終了する（ステップ S 1 3 6）。一方、認証が一致した場合（ステップ S 1 2 4 : Y e s）には、プリンタ 3 0 は印刷クライアント 2 0 に、認証が受け入れられた旨の認証結果を送信する（ステップ S 1 2 8）。

【 0 0 6 1 】

次に、プリンタ 3 0 は、印刷クライアント 2 0 から公開鍵取得要求を受信したかどうかを判断する（ステップ S 1 3 0）。この公開鍵取得要求を受信していない場合（ステップ S 1 3 0 : N o）には、このステップ S 1 3 0 の処理を繰り返して待機する。

【 0 0 6 2 】

公開鍵取得要求を受信した場合（ステップ S 1 3 0 : Y e s）には、プリンタ 3 0 は、E E P R O M 4 5 の公開鍵格納部 E P 1 0 から、公開鍵を読み出して取得する（ステップ S 1 3 2）。続いて、プリンタ 3 0 は、取得した公開鍵を、印刷クライアント 2 0 に送信する（ステップ S 1 3 4）。そして、印刷クライアント 2 0 との接続を終了し（ステップ S 1 3 6）、上述したステップ S 1 2 0 に戻

る。

【0063】

次に、印刷クライアント20が印刷を行いたいときに、その印刷要求をプリンタ30に送信する場合の印刷クライアント20及びプリンタ30の処理について、詳しく説明する。

【0064】

図10は、印刷クライアント20で実行される印刷要求処理を説明するフローチャートである。この印刷要求処理は、印刷クライアントのROM68又はハードディスク76に格納されている印刷要求プログラムをCPU64が読み込んで実行することにより実現される処理である。本実施形態においては、この印刷要求処理は、ユーザが印刷クライアントに印刷指示を入力した場合に、起動され、実行される処理である。

【0065】

この図10に示すように、印刷クライアント20は、ユーザの印刷要求に基づいて、印刷データD05を作成する（ステップS160）。この印刷データD05は、プリンタ30が通常のプリンタである場合に、印刷を実際に行うのに必要となるデータである。

【0066】

次に、印刷クライアント20は、ハードディスク76の公開鍵テーブルTB10から、プリンタ30の公開鍵を読み出す（ステップS162）。続いて、印刷クライアント20は、プリンタ30の公開鍵を用いて、印刷データD05を暗号化して、印刷送信用データD10を生成する（ステップS164）。なお、印刷送信用データD10は、印刷データ以外のデータを含んでいてもよい。

【0067】

次に、印刷クライアント20は、プリンタ30との接続を確立する（ステップS165）。続いて、印刷クライアント20は、この暗号化した印刷送信用データD10を、プリンタ30に送信する（ステップS166）。

【0068】

次に、印刷クライアント20は、プリンタ30から印刷結果情報を受信したか

どうかを判断する（ステップS168）。印刷結果情報を受信していない場合（ステップS168：No）には、このステップS168の処理を繰り返して待機する。一方、印刷結果情報を受信した場合（ステップS168：Yes）には、その印刷結果情報が印刷完了通知であるかどうかを判断する（ステップS170）。

【0069】

この印刷結果情報が印刷完了通知である場合（ステップS170：Yes）には、プリンタ30で印刷が正常に終了したことを意味しているので、ユーザにプリンタ30で印刷が完了した旨を通知する（ステップS172）。一方、受信した印刷結果情報が印刷完了通知でない場合（ステップS170：No）には、その印刷結果情報が解読不能通知であるかどうかを判断する（ステップS174）。

【0070】

印刷結果情報が解読不能通知である場合（ステップS174：Yes）には、ユーザに、プリンタ30で印刷送信用データD10の復号ができなかったため、印刷が行われなかった旨を通知する（ステップS176）。一方、印刷結果情報が解読不能通知でない場合（ステップS174：No）には、その他の何らかのエラーであると考えられるので、ユーザに、そのエラーの種類に応じた通知を行う（ステップS178）。

【0071】

これらステップS172、ステップS176、及び、ステップS178の通知の後、印刷クライアント20は、プリンタ30との接続を切断する（ステップS179）。これにより、この印刷クライアント20における印刷要求処理は終了する。

【0072】

次に、図11に基づいて、印刷クライアント20の印刷要求処理に対応して、プリンタ30で実行される印刷実行処理について説明する。図11は、プリンタ30で実行される印刷実行処理を説明するフローチャートである。この印刷実行処理は、プリンタ30のROM44又はハードディスク58に格納されている印

刷実行プログラムをCPU40が読み込んで実行することにより実現される処理である。本実施形態においては、この印刷実行処理は、一定の時間間隔で定常的に実行されている処理である。

【0073】

図11に示すように、プリンタ30は、印刷クライアント20からの接続を待っており、印刷クライアント20から接続を要求された場合には、プリンタ30は、プリンタケーブル10を介した印刷クライアント20と接続を確立する（ステップS180）。印刷クライアント20と接続が確立した後、プリンタ30は、印刷送信用データD10を受信したかどうかを判断する（ステップS182）。何ら印刷送信用データD10を受信していない場合（ステップS182：No）には、このステップS182の処理を繰り返して待機する。

【0074】

一方、印刷送信用データD10を受信した場合（ステップS182：Yes）には、プリンタ30は自らの機器固有情報を取得する（ステップS184）。続いて、プリンタ30は、位置検出部54から、その時点におけるプリンタ30のプリンタ位置情報を取得する（ステップS186）。このようにプリンタ位置情報を、その都度、位置検出部54から取得することとしているのは、プリンタ30が、公開鍵を登録したときの場所から別の場所に移動された場合には、このプリンタ30で印刷が行われないようにするためである。

【0075】

次に、プリンタ30は、機器固有情報とプリンタ位置情報とに基づいて、パスフレーズを作成する（ステップS188）。このパスフレーズの作成手法は、上述した公開鍵生成処理におけるステップS56と同じ手法である必要がある。なぜなら、パスフレーズが異なると、EEPROM45に格納した公開鍵で暗号化された印刷送信用データを復号できる秘密鍵が、生成できなくなってしまうからである。

【0076】

次に、プリンタ30は、生成したパスフレーズを用いて、公開鍵暗号法により秘密鍵を生成する（ステップS190）。このステップS190で使用するパス

フレーズは、プリンタ 3 0 の設置位置が移動されていなければ、上述した公開鍵生成処理におけるステップ S 5 8 で使用したパスフレーズと同じである。このため、ステップ S 5 8 で生成した公開鍵に対応する秘密鍵が生成される。続いて、プリンタ 3 0 は、生成された秘密鍵を用いて、受信した印刷送信用データ D 1 0 を復号して、印刷データ D 0 5 を取得する（ステップ S 1 9 2）。

【 0 0 7 7 】

次に、プリンタ 3 0 は、秘密鍵を用いて印刷送信用データ D 1 0 の復号ができたかどうかを判断する（ステップ S 1 9 4）。復号ができた場合（ステップ S 1 9 4：Y e s）には、得られた印刷データ D 0 5 に基づいて、印刷エンジン 5 2 を駆動した印刷を実行する（ステップ S 1 9 6）。具体的には、印刷データ D 0 5 の言語解釈を行い、印刷エンジン 5 2 に適合した印刷要求データを生成する。そして、この印刷要求データを印刷エンジン 5 2 に送信することにより、印刷エンジン 5 2 で印刷用紙等に印刷が行われる。

【 0 0 7 8 】

この印刷が正常に完了した時点で、プリンタ 3 0 は、印刷が正常に終了した旨の印刷完了通知を、印刷結果情報として、印刷クライアント 2 0 に送信する（ステップ S 1 9 8）。

【 0 0 7 9 】

これに対して、ステップ S 1 9 4 において、印刷送信用データ D 1 0 の復号ができなかったと判断した場合（ステップ S 1 9 4：N o）には、解読不能通知を印刷結果情報として、印刷クライアント 2 0 に送信する（ステップ S 2 0 0）。

【 0 0 8 0 】

これらステップ S 1 9 8 又はステップ S 2 0 0 の後、プリンタ 3 0 は、印刷クライアント 2 0 との接続を終了する（ステップ S 2 0 2）。そして、上述したステップ S 1 8 0 の処理に戻る。

【 0 0 8 1 】

以上のように、本実施形態に係る印刷システムによれば、プリンタ 3 0 は、正当な権限を有する者が指示をした場合に限り、公開鍵を生成して、E E P R O M 4 5 に登録できるようにしたので、プリンタ 3 0 が正常な印刷をできる設置位置

を限定することができる。

【0082】

すなわち、プリンタ30は、正当な権限を有する操作者が公開鍵の生成をプリンタ30に要求した場合には、プリンタ30は、その時点におけるプリンタ位置情報を含むパズフレーズを用いて、公開鍵を生成し、EEPROM45に格納する。一方、正当な権限を有する操作者でない場合には、プリンタ30は、公開鍵を生成しない。そして、プリンタ30が印刷クライアント20に公開鍵を送信する場合には、EEPROM45に格納されている公開鍵を読み出して、送信する。

【0083】

印刷クライアント20がプリンタ30に印刷データD05を送信する際には、この公開鍵を用いて暗号化した印刷送信用データD10として送信する。プリンタ30では、印刷送信用データD10を受信する都度、その時点におけるプリンタ位置情報を取得し、このプリンタ位置情報を含むパズフレーズを用いて秘密鍵を生成する。そして、プリンタ30は、この秘密鍵で印刷送信用データD10を復号し、復号できた場合は印刷を行い、復号できなかった場合には印刷を行わない。このため、EEPROM45に公開鍵を格納した際のプリンタ位置情報と、秘密鍵を生成する際のプリンタ位置情報が異なると、受信した印刷送信用データD10の復号が適正にできないこととなり、正常な印刷結果を得ることができない。これにより、プリンタ30が使用できる位置を、正当な権限を有する者が、プリンタ30に公開鍵の生成を指示した場所に限定することができる。

【0084】

また、正当な権限を有する操作者であれば、EEPROM45に格納されている公開鍵を変更することができるので、プリンタメーカ等の正当な理由でプリンタ30の設置場所を変更する場合でも、このプリンタ30を引き続き、使用することができる。すなわち、正当な権限を有する操作者が、プリンタ30の新たな設置場所で、再度、プリンタ30に公開鍵の生成を指示すれば、その場所のプリンタ位置情報に基づいて、新たな公開鍵が生成され、EEPROM45に格納される。このため、プリンタ30を有効に活用することができるようになる。

【0085】

〔第2実施形態〕

第2実施形態は、上述した第1実施形態を変形して、プリンタ30が公開鍵の代わりにプリンタ位置情報をEEPROM45に格納しておくようにしたものである。より詳しくを、以下に説明する。

【0086】

なお、本実施形態に係る印刷システムの構成は、上述した第1実施形態における図1と同様であり、プリンタ30の構成は、上述した図2と同様であり、印刷クライアント20の構成は、上述した図3と同様である。また、本実施形態に係る公開鍵要求処理、印刷要求処理、及び、印刷実行処理も、上述した第1実施形態と同様である。

【0087】

但し、本実施形態に係るプリンタ30では、公開鍵生成処理の代わりに、プリンタ位置情報登録処理が実行される。

【0088】

図12は、本実施形態に係るプリンタ30が実行するプリンタ位置情報登録処理を説明するフローチャートを示す図である。このプリンタ位置情報登録処理は、プリンタ30のROM44又はハードディスク58に格納されているプリンタ位置情報登録プログラムをCPU40が読み込んで実行することにより実現される処理である。また、本実施形態においては、このプリンタ位置情報登録処理は、操作者（例えば、プリンタ30のメーカーのメンテナンスをする者）がプリンタ30のコントロールパネルを操作して、プリンタ位置情報登録処理を実行するように指示した場合に、起動され、実行される処理である。

【0089】

この図12に示すように、公開鍵生成処理が実行された場合、プリンタ30はまず、操作者に、プリンタ位置情報登録認証情報を入力するように要求する（ステップS206）。本実施形態においては、操作者は、プリンタ30のコントロールパネルから、IDとパスワードをプリンタ位置情報登録認証情報として入力する。

【0090】

次に、プリンタ30は、プリンタ位置情報登録認証情報が入力されたかどうかを判断する（ステップS208）。このプリンタ位置情報登録認証情報が入力されていない場合（ステップS208：No）には、ステップS208の処理を繰り返して待機する。

【0091】

一方、プリンタ位置情報登録認証情報が入力された場合（ステップS208：Yes）には、入力されたプリンタ位置情報登録認証情報が、登録されているプリンタ位置情報登録認証情報と一致するかどうかを判断する（ステップS210）。本実施形態においては、登録されたプリンタ位置情報登録認証情報は、ROM44、EEPROM45、又は、ハードディスク58などに予め格納されている。このため、プリンタ30は、格納されているプリンタ位置情報登録認証情報を読み出して、操作者が入力したプリンタ位置情報登録認証情報と一致するかどうかを判断する。具体的には、登録されているID及びパスワードが、操作者が入力したID及びパスワードと一致するかどうかを判断する。

【0092】

プリンタ位置情報登録認証情報が一致しなかった場合（ステップS210：No）には、新たにプリンタ位置情報を登録を生成することなく、このプリンタ位置情報登録処理を終了する。

【0093】

一方、プリンタ位置情報登録認証情報が一致した場合（ステップS210：Yes）には、プリンタ30は位置検出部54から、その時点におけるプリンタ30のプリンタ位置情報を取得する（ステップS212）。これにより、プリンタ30のその時点における設置位置に関する情報を取得することができる。

【0094】

次に、プリンタ30は、この取得したプリンタ位置情報を、EEPROM45に格納する（ステップS214）。図13は、EEPROM45の一部の領域に形成されるプリンタ位置情報格納部EP20の構成を示す図である。この図13に示すように、プリンタ位置情報格納部EP20に、取得したプリンタ位置情報

を格納して、保持する。

【0095】

これにより、本実施形態に係るプリンタ位置情報登録処理が終了する。

【0096】

図14及び図15は、本実施形態に係る公開鍵送信処理を説明するフローチャートである。図14に示すように、本実施形態に係る公開鍵送信処理は、ステップS130までは上述した第1実施形態と同様である。

【0097】

このステップS130の後、本実施形態に係る公開鍵送信処理では、プリンタ30は、機器固有情報を取得する（ステップS218）。ここで、機器固有情報とは、上述した第1実施形態と同様であり、このプリンタ30に関して、固有に割り当てられている識別情報であり、例えば、プリンタ30の製造シリアルナンバー、MACアドレス等がある。

【0098】

次に、図15に示すように、プリンタ30は、EEPROM45から、プリンタ位置情報格納部EP20に格納されているプリンタ位置情報を読み出す（ステップS220）。すなわち、本実施形態においては、公開鍵の送信を印刷クライアント20から要求される都度、秘密鍵暗号法により公開鍵を生成するが、そのパズフレーズに使用するプリンタ位置情報は、固定的なものになる。このため、公開鍵を生成する度に、同じ公開鍵が得られることとなる。

【0099】

次に、プリンタ30は、機器固有情報とプリンタ位置情報とを用いてパズフレーズを作成する（ステップS222）。このパズフレーズの作成手法は種々のものが考えられるが、本実施形態においては、単純に機器固有情報の後ろにプリンタ位置情報をつなげることにより、パズフレーズを作成する。なお、パズフレーズは、これら機器固有情報及びプリンタ位置情報以外のデータを含んでいてもよい。

【0100】

次に、プリンタ30は、ステップS222で作成したパズフレーズを用いて、

公開鍵暗号法により、公開鍵を生成する（ステップ S 2 2 4）。続いて、プリンタ 3 0 は、この生成した公開鍵を印刷クライアント 2 0 に送信する（ステップ S 2 2 6）。そして、印刷クライアント 2 0 との接続を終了し（ステップ S 2 2 8）、図 1 4 のステップ S 1 2 0 に戻る。

【0 1 0 1】

以上のように、本実施形態に係る印刷システムによれば、プリンタ 3 0 は、正当な権限を有する者が指示をした場合に限り、その時点のプリンタ位置情報を E E P R O M 4 5 に格納するようにしたので、プリンタ 3 0 が正常な印刷をできる設置位置を限定することができる。

【0 1 0 2】

すなわち、プリンタ 3 0 は、正当な権限を有する操作者が新たなプリンタ位置情報の登録を要求した場合には、プリンタ 3 0 は、その時点におけるプリンタ位置情報を E E P R O M 4 5 に格納する。一方、正当な権限を有する操作者でない場合には、プリンタ 3 0 は、プリンタ位置情報を E E P R O M 4 5 に格納しない。そして、プリンタ 3 0 が印刷クライアント 2 0 に公開鍵を送信する場合には、E E P R O M 4 5 に格納されているプリンタ位置情報を少なくとも含むパスフレーズを用いて公開鍵を生成し、送信する。

【0 1 0 3】

印刷クライアント 2 0 がプリンタ 3 0 に印刷データ D 0 5 を送信する際には、この公開鍵を用いて暗号化した印刷送信用データ D 1 0 として送信する。プリンタ 3 0 では、印刷送信用データ D 1 0 を受信する都度、その時点におけるプリンタ位置情報を取得し、このプリンタ位置情報を含むパスフレーズを用いて秘密鍵を生成する。そして、プリンタ 3 0 は、この秘密鍵で印刷送信用データ D 1 0 を復号し、復号できた場合は印刷を行い、復号できなかった場合には印刷を行わない。このため、E E P R O M 4 5 に格納したプリンタ位置情報と、秘密鍵を生成する際のプリンタ位置情報が異なると、受信した印刷送信用データ D 1 0 の復号が適正にできないこととなり、正常な印刷結果を得ることができない。これにより、プリンタ 3 0 が使用できる位置を、正当な権限を有する者が、プリンタ 3 0 にプリンタ位置情報の登録した場所に限定することができる。

【0104】

また、正当な権限を有する操作者であれば、EEPROM45に格納されているプリンタ位置情報を変更することができるので、プリンタメーカ等の正当な理由でプリンタ30の設置場所を変更する場合でも、このプリンタ30を引き続き、使用することができる。すなわち、正当な権限を有する操作者が、プリンタ30の新たな設置場所で、再度、プリンタ30にプリンタ位置情報の登録を指示すれば、その場所のプリンタ位置情報がEEPROM45に格納される。このため、プリンタ30を有効に活用することができるようになる。

【0105】

なお本発明は上記実施形態に限定されずに種々に変形可能である。例えば、上述した第1実施形態においては、正当な権限を有する操作者であるかどうかを示す公開鍵生成認証情報をIDとパスワードの組み合わせで構成し、第2実施形態においては、正当な権限を有する操作者であるかどうかを示すプリンタ位置情報登録認証情報をIDとパスワードの組み合わせで構成したが、公開鍵生成認証情報及びプリンタ位置情報登録認証情報は、IDとパスワードの組み合わせに限るものではない。例えば、プリンタ30に、正当な権限を有する者の指紋を登録しておき、操作者の指紋を読み取って、指紋が一致した場合に、正当な権限を有する者であると判断するようにしてもよい。

【0106】

また、使用できる位置を制限するデータ受信装置としてプリンタを例示して説明したが、本発明はプリンタに限定されるものではない。さらに、データ送信装置も、印刷クライアントに限定されるものではない。

【0107】

例えば、データ送受信システムにおけるデータ送信装置が画像撮影用のデジタルカメラであり、データ受信装置がデジタルカメラで撮影した画像データを蓄積するデータサーバであってもよい。この場合、デジタルカメラから送信されるデータはデータサーバから受信した公開鍵を用いて暗号化されており、このデータを受信したデータサーバでは、上述した手法により秘密鍵を生成し、このデータの復号を行うこととなる。そして、受信したデータの復号ができた場合には、そ

のデータを蓄積し、復号できなかった場合には、そのデータを蓄積しないこととなる。

【0108】

また、データ送受信システムにおけるデータ送信装置がパーソナルコンピュータであり、データ受信装置がそのパーソナルコンピュータから送信された画像データを投影するプロジェクタであってもよい。この場合、パーソナルコンピュータから送信されるデータはプロジェクタから受信した公開鍵を用いて暗号化されており、このデータを受信したプロジェクタでは、上述した手法により秘密鍵を生成し、このデータの復号を行うこととなる。そして、受信したデータの復号ができた場合には、そのデータを投影し、復号できなかった場合には、そのデータを投影しないこととなる。

【0109】

さらには、データ送受信システムにおけるデータ送信装置が音楽等のコンテンツサーバであり、データ受信装置がコンテンツサーバから送信された音楽等のコンテンツデータの再生装置であってもよい。この場合、コンテンツサーバから送信されるデータは再生装置から受信した公開鍵を用いて暗号化されており、このデータを受信した再生装置では、上述した手法により秘密鍵を生成し、このデータの復号を行うこととなる。そして、受信したデータの復号ができた場合には、そのデータを再生し、復号できなかった場合には、そのデータを再生しないこととなる。

【0110】

また、上述した実施形態では、プリンタ30の印刷媒体が印刷用紙である場合を例に説明したが、印刷媒体はこれに限るものではなく、例えば、OHPシート等の他の印刷媒体であっても本発明を適用することができる。

【0111】

さらに、上述の実施形態で説明した各処理については、これら各処理を実行するためのプログラムをフレキシブルディスク、CD-ROM (Compact Disc-Read Only Memory)、ROM、メモリカード等の記録媒体に記録して、記録媒体の形で頒布することが可能である。この場合、このプログラムが記録された記録媒

体を印刷クライアント 2 0 及び／又はプリンタ 3 0 に読み込ませ、実行させることにより、上述した実施形態を実現することができる。

【0 1 1 2】

また、印刷クライアント 2 0 及び／又はプリンタ 3 0 は、オペレーティングシステムや別のアプリケーションプログラム等の他のプログラムを備える場合がある。この場合、印刷クライアント 2 0 及び／又はプリンタ 3 0 の備える他のプログラムを活用し、記録媒体には印刷クライアント 2 0 及び／又はプリンタ 3 0 が備えるプログラムの中から、上述した実施形態と同等の処理を実現するプログラムを呼び出すような命令を記録するようにしてもよい。

【0 1 1 3】

さらに、このようなプログラムは、記録媒体の形ではなく、ネットワークを通じて搬送波として頒布することも可能である。ネットワーク上を搬送波の形で伝送されたプログラムは、印刷クライアント 2 0 及び／又はプリンタ 3 0 に取り込まれて、このプログラムを実行することにより上述した実施形態を実現することができる。

【0 1 1 4】

また、記録媒体にプログラムを記録する際や、ネットワーク上を搬送波として伝送される際に、プログラムの暗号化や圧縮化がなされている場合がある。この場合には、これら記録媒体や搬送波からプログラムを読み込んだ印刷クライアント 2 0 及び／又はプリンタ 3 0 は、そのプログラムの復号や伸張を行った上で、実行する必要がある。

【0 1 1 5】

【発明の効果】

以上説明したように、本発明に係るプリンタ及び印刷システムによれば、プリンタが印刷を行える位置を、所定の場所に制限することができる。

【図面の簡単な説明】

【図 1】

本発明の第 1 実施形態に係る印刷システムの構成の一例を示す図。

【図 2】

本発明の第 1 実施形態に係るプリンタのハードウェア構成の一例を示す図。

【図 3】

本発明の第 1 実施形態に係る印刷クライアントの構成の一例を示す図。

【図 4】

本発明の第 1 実施形態において、公開鍵と秘密鍵とを用いた、印刷データの暗号化と復号を説明するための概念図。

【図 5】

本発明の第 1 実施形態に係るプリンタが実行する公開鍵生成手段を説明するフローチャートを示す図。

【図 6】

本発明の第 1 実施形態に係るプリンタの E E P R O M に形成される公開鍵格納部の構成を示す図。

【図 7】

本発明の第 1 実施形態に係る印刷クライアントが実行する公開鍵要求処理を説明するフローチャートを示す図。

【図 8】

本発明の第 1 実施形態に係る印刷クライアントが備える公開鍵テーブルの構成の一例を示す図。

【図 9】

本発明の第 1 実施形態に係るプリンタが実行する公開鍵送信処理を説明するフローチャートの一部を示す図。

【図 1 0】

本発明の第 1 実施形態に係る印刷クライアントが実行する印刷要求処理を説明するフローチャートを示す図。

【図 1 1】

本発明の第 1 実施形態に係るプリンタが実行する印刷実行処理を説明するフローチャートを示す図。

【図 1 2】

本発明の第 2 実施形態に係るプリンタが実行するプリンタ位置情報登録処理を

説明するフローチャートを示す図。

【図 13】

本発明の第2実施形態に係るプリンタのEEPROMに形成される公プリンタ位置情報格納部の構成を示す図。

【図 14】

本発明の第2実施形態に係るプリンタが実行する公開鍵送信処理を説明するフローチャートの一部を示す図（その1）。

【図 15】

本発明の第1実施形態に係るプリンタが実行する公開鍵送信処理を説明するフローチャートの一部を示す図（その2）。

【符号の説明】

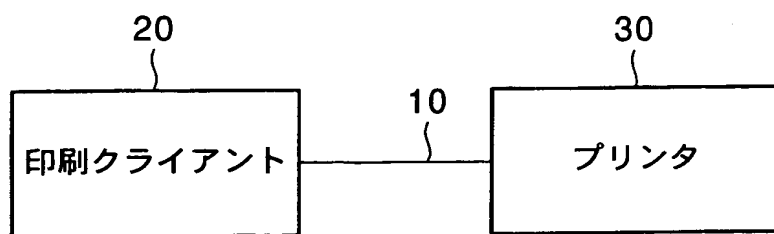
- 10 ネットワーク
- 20 印刷クライアント
- 30 プリンタ
- 40 CPU
- 42 RAM
- 44 ROM
- 45 EEPROM
- 46 内部バス
- 48、50、56 インターフェース
- 52 印刷エンジン
- 54 位置検出部
- 58 ハードディスク
- 60 コンピュータ本体
- 62 ディスプレイ
- 64 CPU
- 66 RAM
- 68 ROM
- 70 内部バス

7 2、7 4、7 8 インターフェース

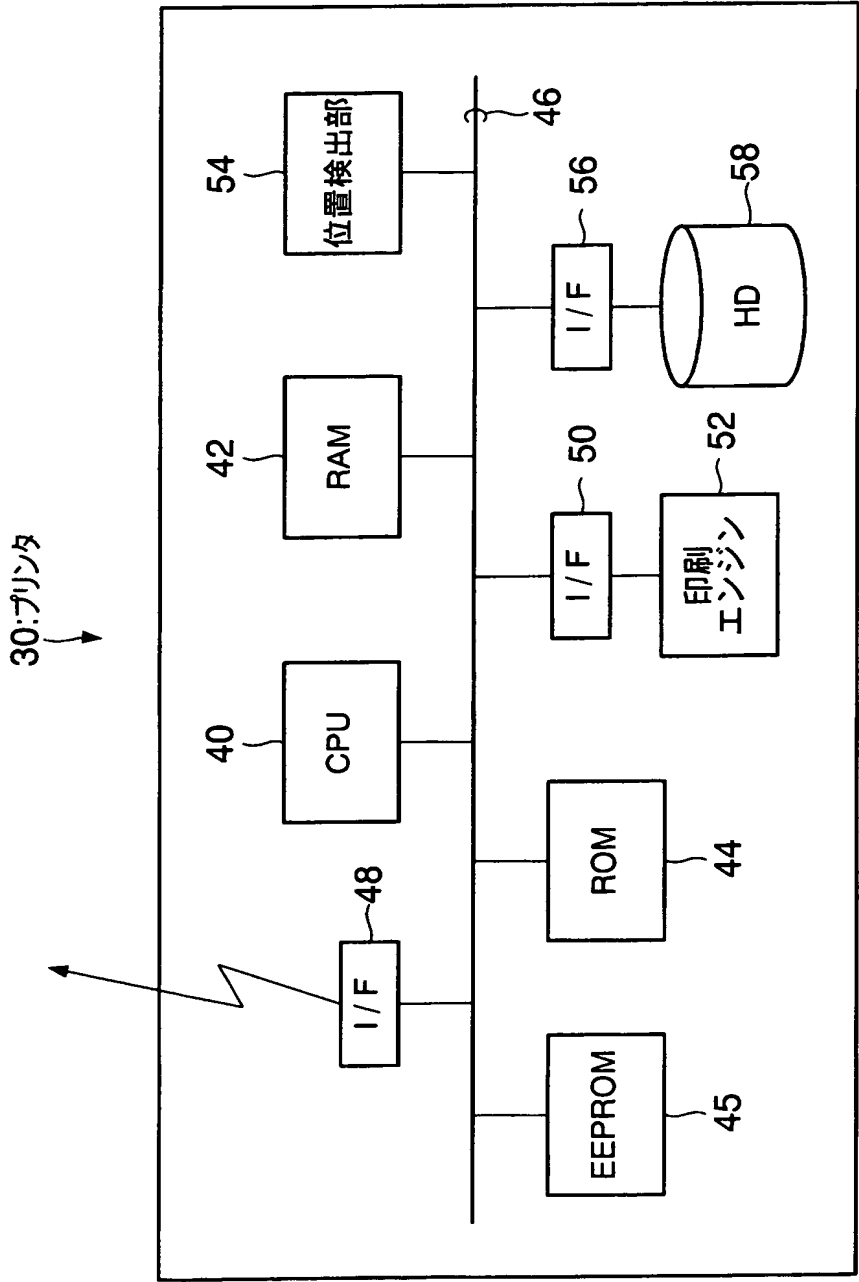
7 6 ハードディスク

【書類名】 図面

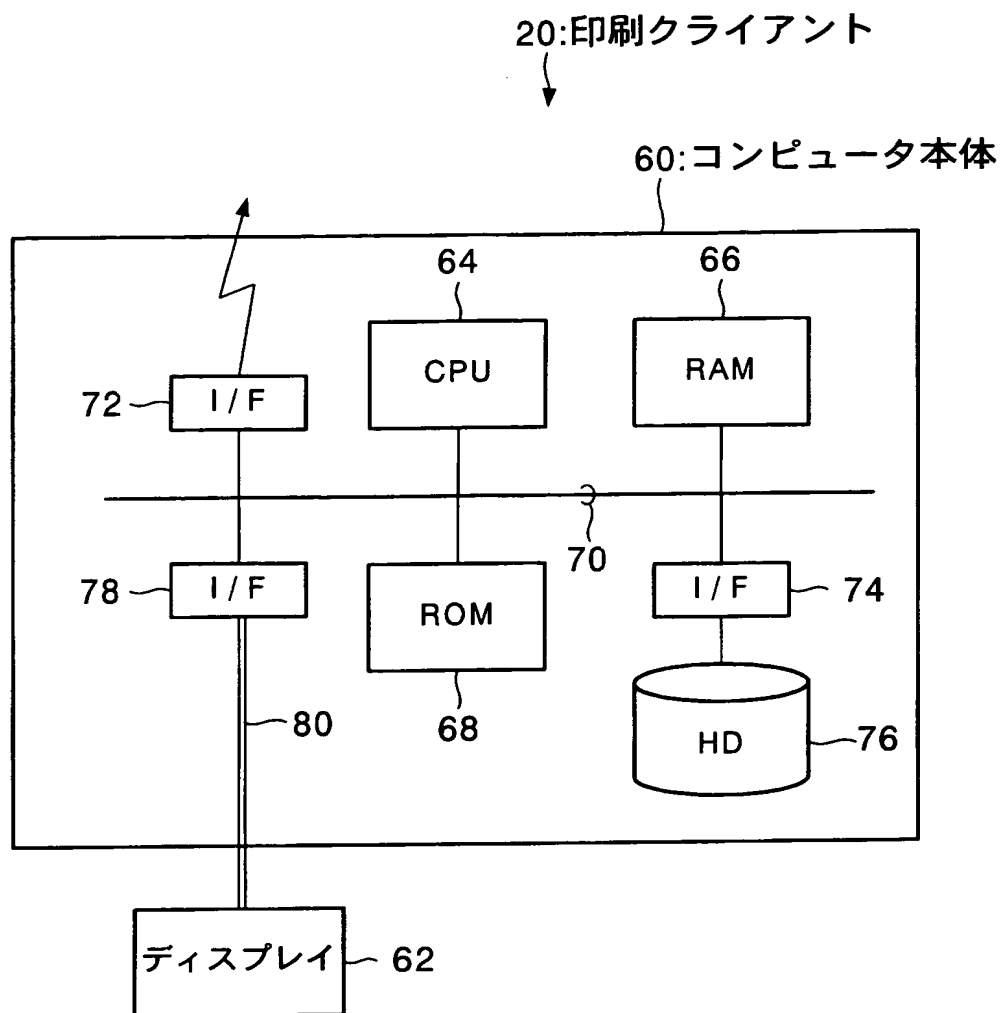
【図 1】



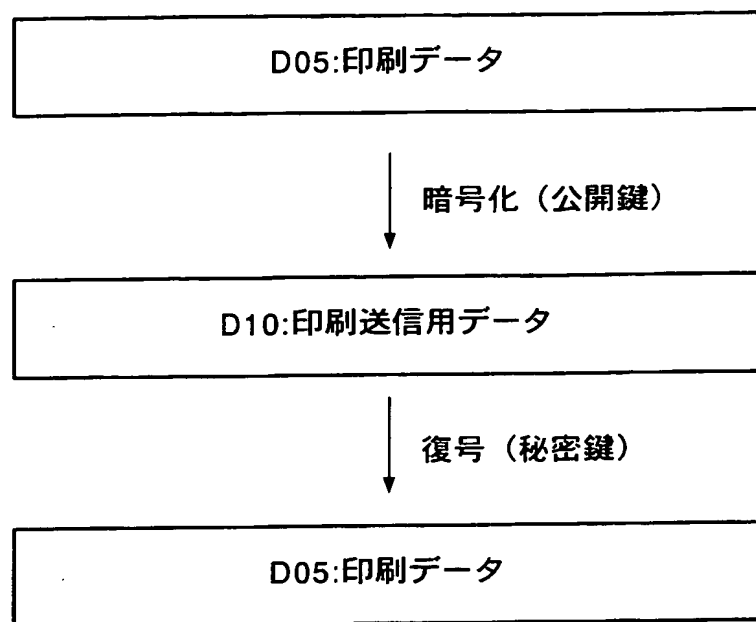
【図 2】



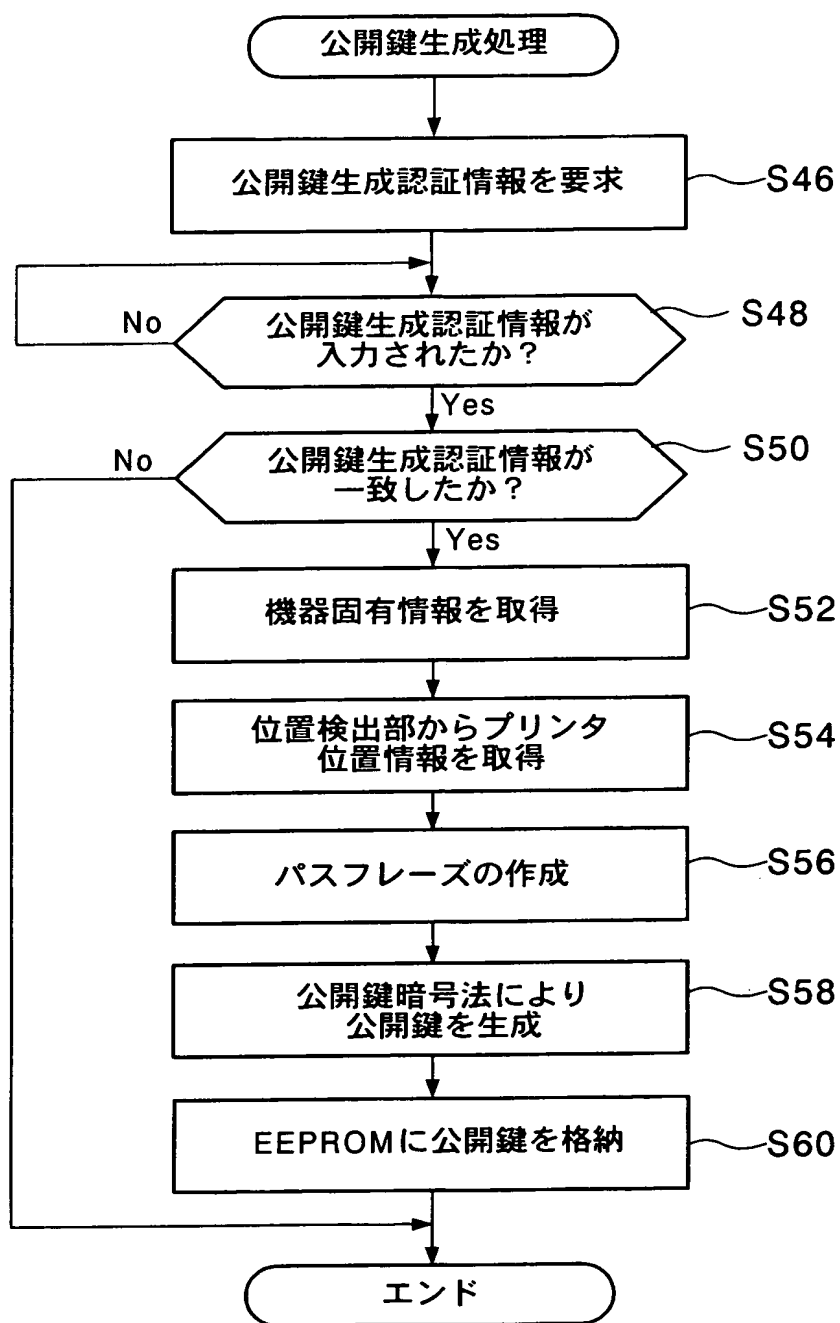
【図 3】



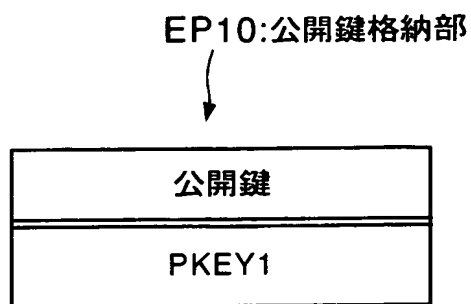
【図 4】



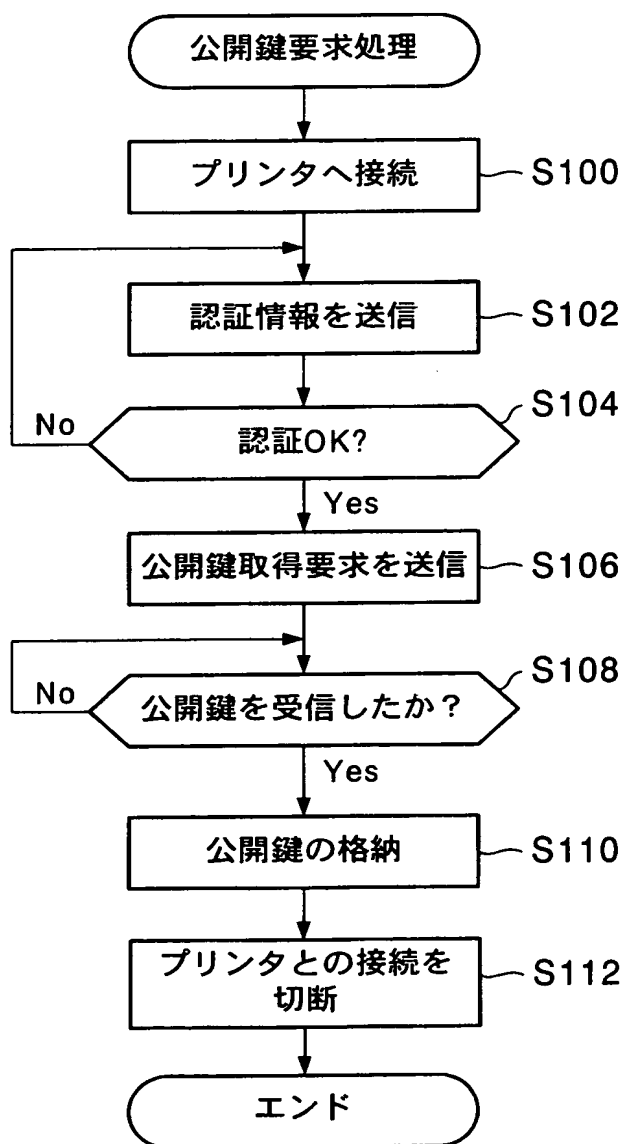
【図 5】



【図 6】



【図 7】



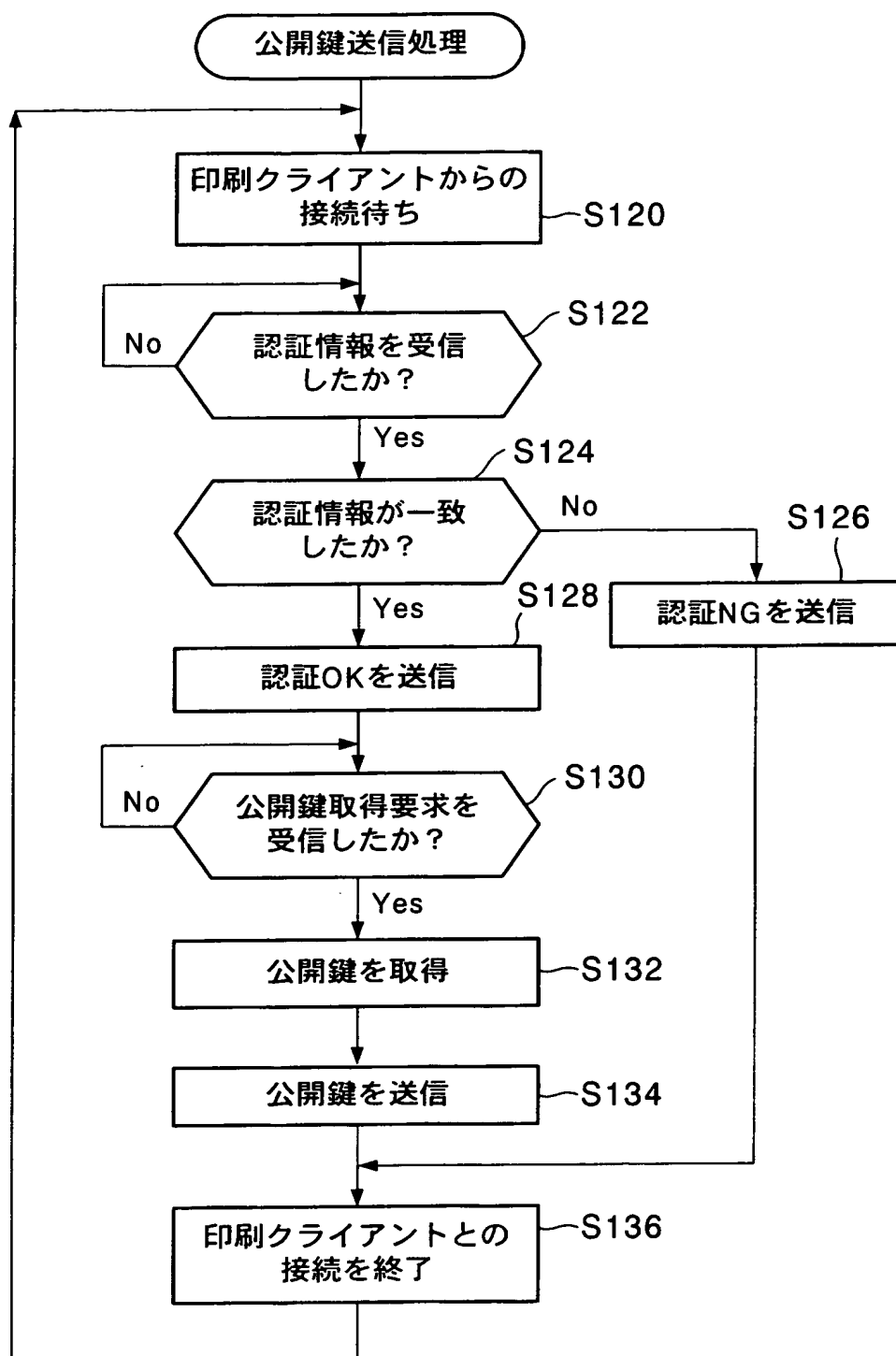
【図 8】

TB10: 公開鍵テーブル

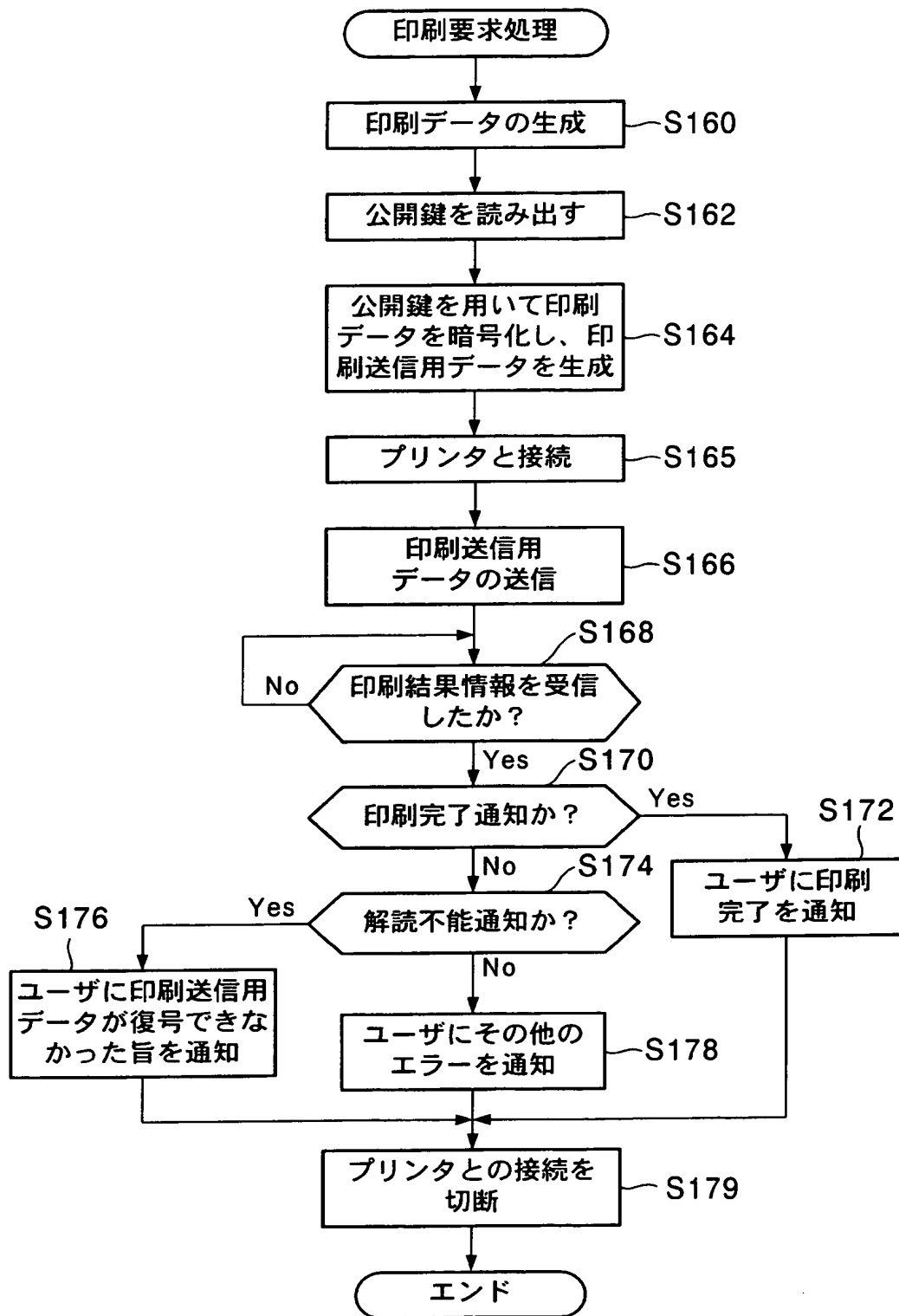


TD10 プリンタ	TD11 公開鍵
PRINTER-ID1	PKEY1
PRINTER-ID2	PKEY2
⋮	⋮

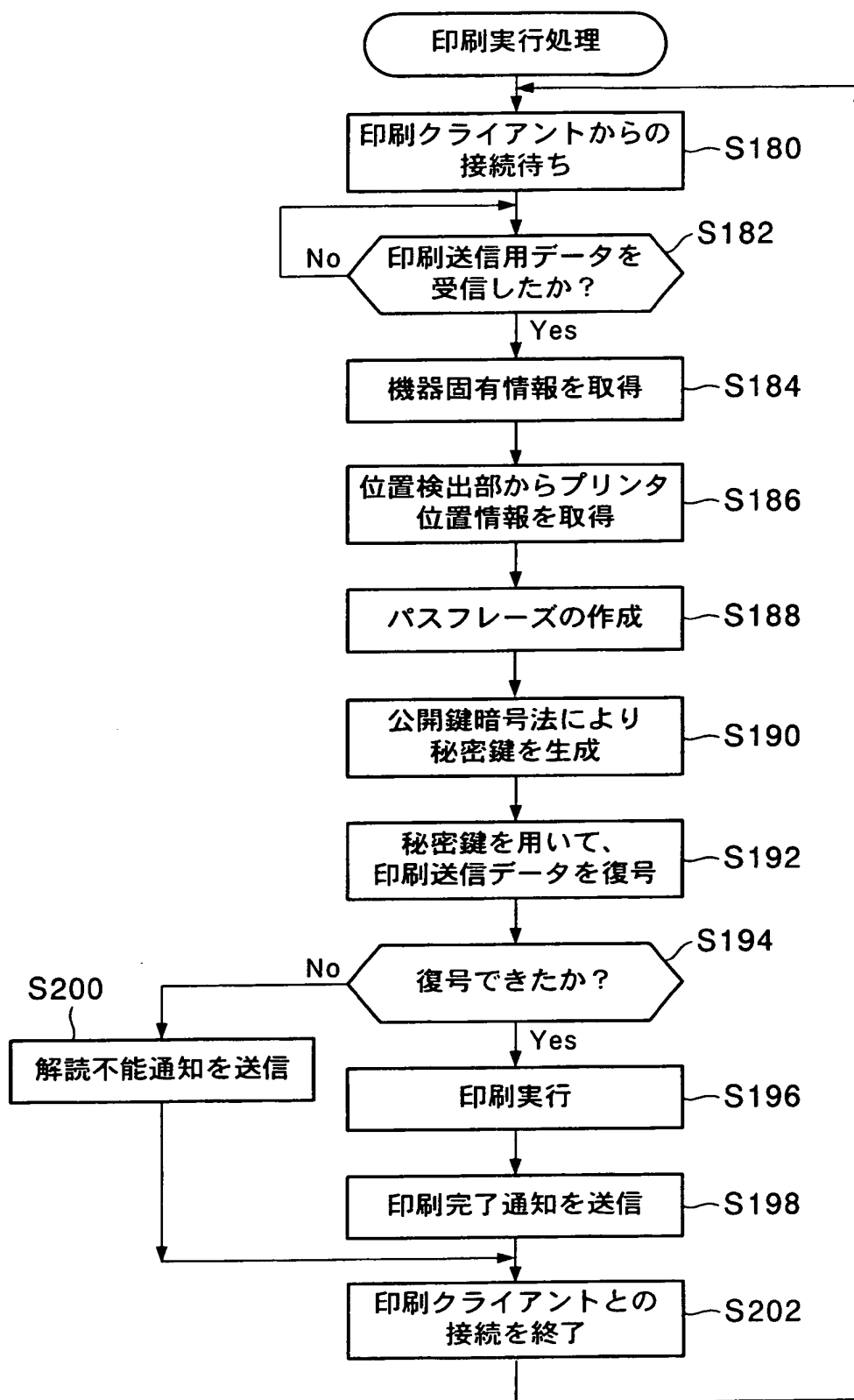
【図 9】



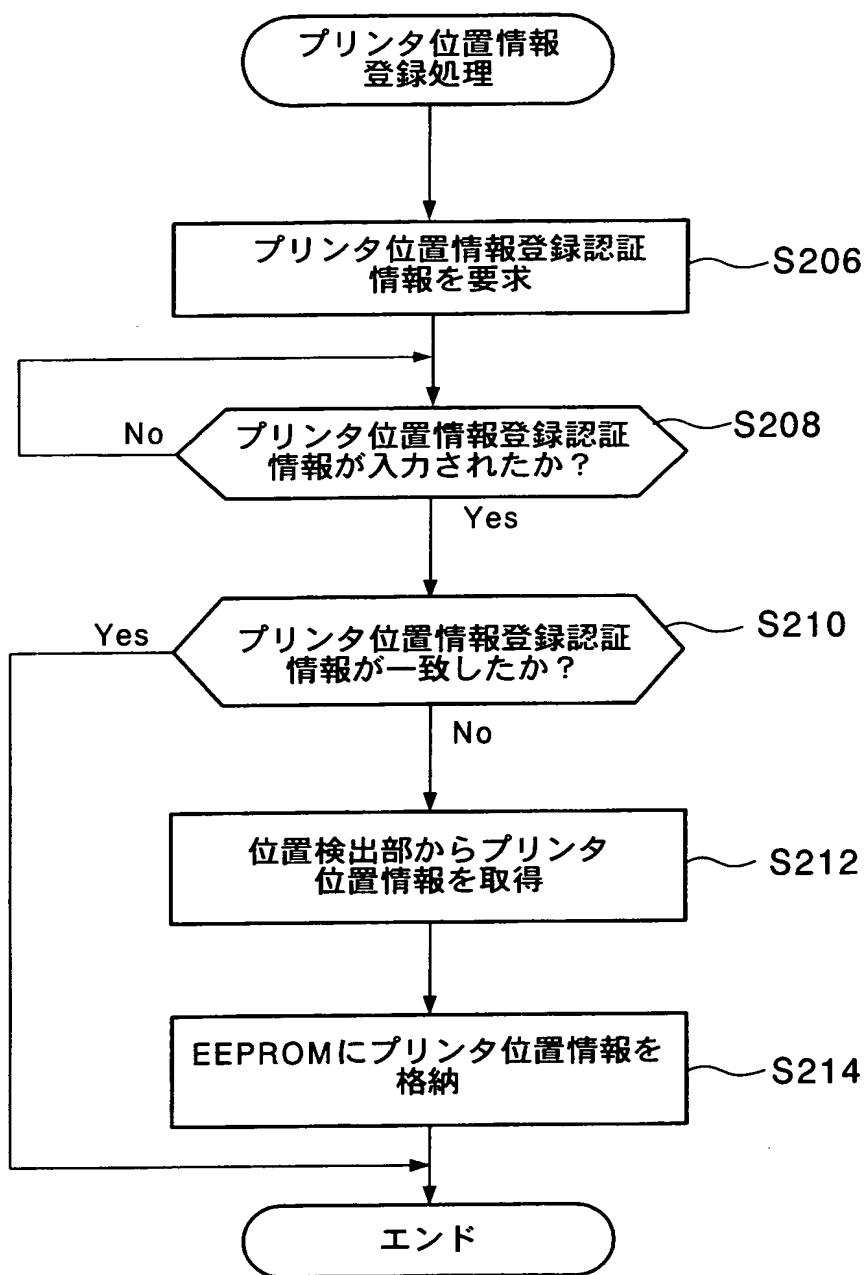
【図 10】



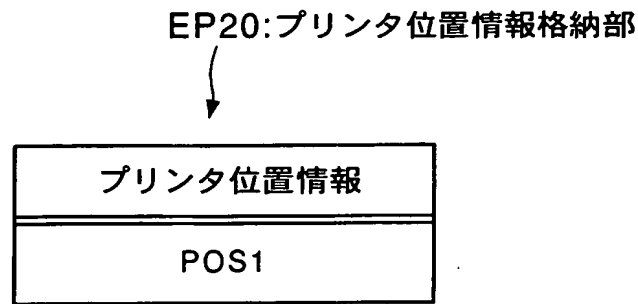
【図 11】



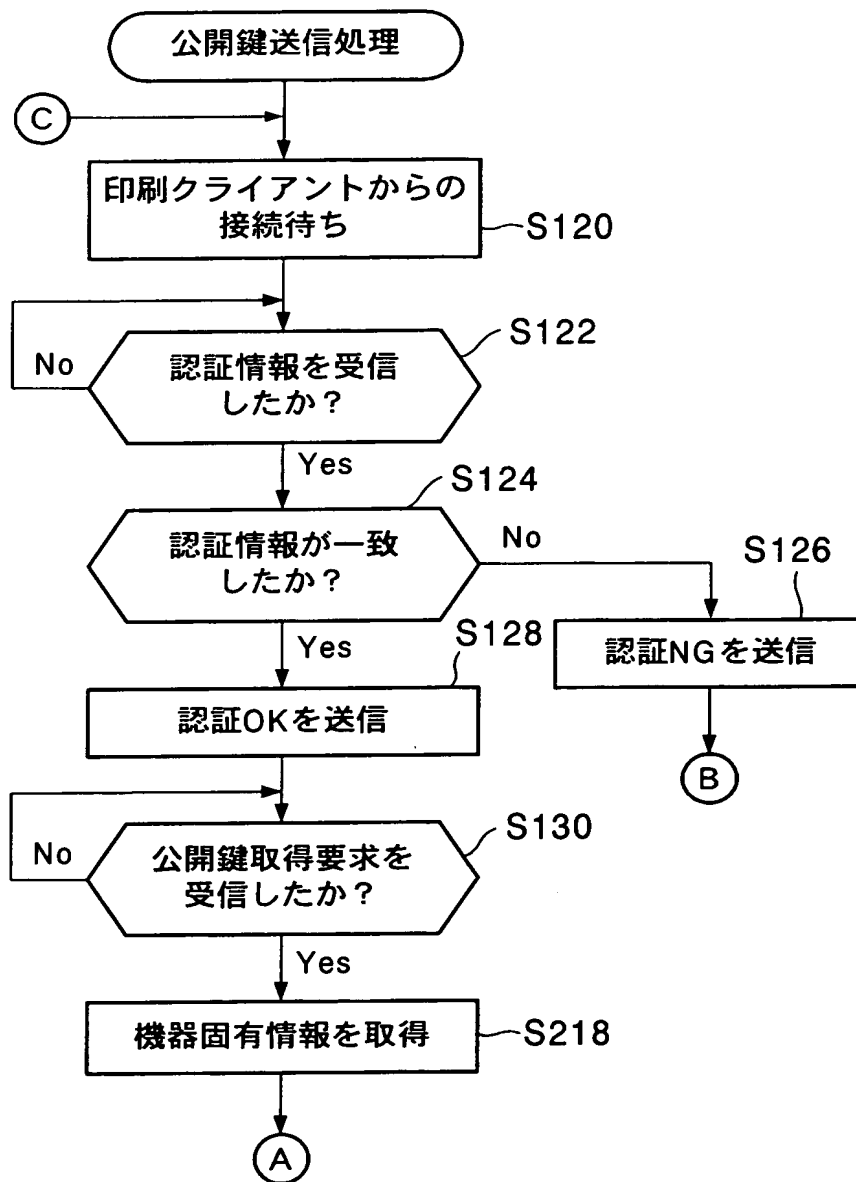
【図 12】



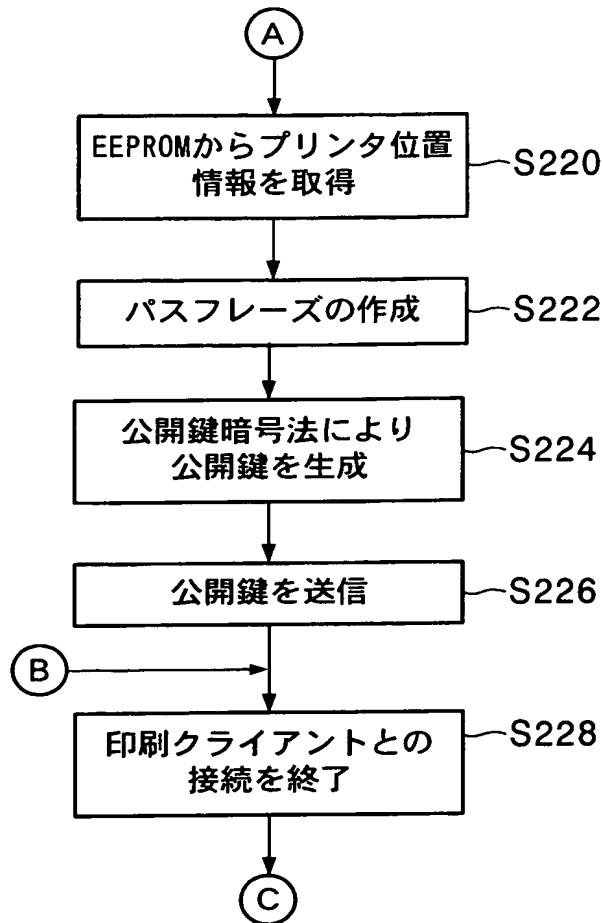
【図 13】



【図 14】



【図 15】



【書類名】 要約書

【要約】

【課題】 プリンタ 3 0 が使用できる位置に制限をかける。

【解決手段】 プリンタ 3 0 は、正当な権限を有する操作者が指示した場合に限り、少なくともプリンタ位置情報を含むパスフレーズを用いて、公開鍵暗号法により、公開鍵を生成し、この公開鍵を公開鍵格納部 E P 1 0 に格納する。印刷クライアント 2 0 から公開鍵の送信を要求された場合には、プリンタ 3 0 は公開鍵格納部 E P 1 0 から公開鍵を読み出して、印刷クライアント 2 0 に送信する。印刷クライアント 2 0 がプリンタ 3 0 に印刷データ D 0 5 を送信する場合には、印刷データ D 0 5 を予め取得した公開鍵を用いて暗号化して、印刷送信用データ D 1 0 として送信する。この印刷送信用データ D 1 0 を受信したプリンタ 3 0 は、少なくともプリンタ位置情報を含むパスフレーズを用いて、公開鍵暗号法により、秘密鍵を生成する。そして、この秘密鍵を用いて、受信した印刷送信用データ D 1 0 を復号する。このため、プリンタ 3 0 が公開鍵を生成した時のプリンタ位置情報と、秘密鍵を生成する時のプリンタ位置情報とが異なると、印刷送信用データ D 1 0 の復号ができなくなる。

【選択図】 図 1

特願 2 0 0 2 - 3 4 3 8 7 3

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 2 3 6 9]

1. 変更年月日

1 9 9 0 年 8 月 2 0 日

[変更理由]

新規登録

住 所

東京都新宿区西新宿 2 丁目 4 番 1 号

氏 名

セイコーエプソン株式会社